UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**STIPULATION OF**
Manning, Bradley E.	)	**EXPECTED TESTIMONY**
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	**Mr. Sean Chamberlin**
Joint Base Myer-Henderson Hall	)	
Fort Myer, Virginia 22211	)	9 **June 2013**

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Sean Chamberlin were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I am a Systems Administrator for the S6 shop of the 902d Military Intelligence (MI) Group on Fort Meade, Maryland. The 902d MI Group performs counterintelligence functions. My section is responsible for providing IT support for all unit servers. In this capacity, I build new servers and maintain old ones. I have worked in this capacity for ten years. Before that I was active duty military for nine years and was a Staff Sergeant when I left the Army. For the last five of my nine years of active duty service, I had the Military Occupational Specialty (MOS) 33W, which is Intercept Electronic Warfare Systems Repair. In that capacity, I was a systems administrator. To fulfill my current function, I have received Security Plus training and have certifications in numerous Microsoft server types. I also hold a Bachelor's degree in Information Systems from the University of Phoenix.

2. I first became involved in the present case in July of 2011 when my supervisor Mr. Robert Conner, the Site Lead for Information Technology at the 902d MI Group, requested that I pull Microsoft Internet Information Services (MIIS) web server audit event logs for the contacting IP addresses 22.225.41.22 and 22.225.41.40 between the dates November 2009 and May 2010. MIIS are application logs that are specific to the web server. Audit logs are a record of the activity that occurs on the server and enable system administrators like me to track what users do on the website. Audit logs contain data that is automatically written to them on a daily basis. Here, the audit logs record file activity on a web server from the United States Government computer assigned to the IP address 199.32.48.154, is a computer dedicated to processing classified information at the SECRET level. This is the IP address for the ACIC website on SIPRNET.

3. This data shows what IP addresses accessed our system within that date range. An IP address is part of the Transmission Control Protocol/Internet Protocol (TCP/IP). A protocol is the standard language used to communicate over a network. TCP/IP is the most common "language" that computers use to communicate over the Internet. An IP address is the method of identifying a specific computer on a network.

4. An IP address allows us to know which computer on a given network accessed our server. In this case, I pulled eighteen log files for the above IP address and date range. The files are named the following: ex091119.log; ex091201.log; ex091214.log; ex091217.log; ex091221.log; ex091229.log; ex100207.log; ex100209.log; ex100211.log; ex100214.1og; ex100301.log;

/02

PROSECUTION EXHIBIT 71 for identification
PAGE OFFERED:___ PAGE ADMITTED:___
PAGE 1 OF 2 PAGES

ex100302.1og; ex100308.log; ex100315.log; ex100316.log; ex100317.log, which is the automatic naming convention of Microsoft based on date. The files display in text format. The files contain 86 entries for the IP address of 22.225.41.22 and 28 entries for the IP address of 22.225.41.40. The first entry for 22.225.41.22 or 22.225.41.40 is 19 November ~~2010.~~ 2009. TH BEM KF

5. These logs are on our external web server, which is one of the servers I am responsible for maintaining. The web server and the logs are located in what is commonly referred to as the "DMZ", which is the area between our internal system and the SIPRNET. I pulled the data using a search window and searching the IP address for the given date range. Then I searched for the two requested IP addresses. I then put the files into an internal investigation folder and had them burned to a disc. I looked at the disc to verify that they were the logs that I pulled.

6. I am familiar with these logs because of my work as a systems administrator. After I pulled the logs, they were burned onto a rewritable disc by another individual. I reviewed the contents of the disc to ensure it contained the logs that I pulled. The disc labeled "Log Files 902nd MI 2011-0006" contain the logs that I pulled. **Prosecution Exhibit 64 for Identification** is a copy of this disc. I attested to the authenticity of these logs on 21 June 2012 (BATES number: 00449439). I pulled the logs from the server and did not alter the content of the logs in any way. I have no reason to believe anyone else would have modified the logs in any way while they are on the server as permissions to the "DMZ" are very limited.

	Thomas F. Hurley	
ANGEL M. OVERGAARD CPT, JA Assistant Trial Counsel	THOMAS HURLEY MAJ, JA Defense Counsel	BRADLEY E. MANNING PFC, USA Accused